CJCSI 6722.01
1 July 1997

GLOBAL COMMAND AND CONTROL SYSTEM CONFIGURATION MANAGEMENT POLICY

JOINT STAFF
WASHINGTON, D.C. 20318-0400

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6722.01
DISTRIBUTION: A,B,C,J,S 1 July 1997

GLOBAL COMMAND AND CONTROL SYSTEM
CONFIGURATION MANAGEMENT
POLICY

References: See Enclosure E

1. Purpose. This instruction defines the configuration management (CM) policy for the Global Command and Control System (GCCS) and outlines a joint level CM structure for effecting orderly, controlled changes to the operational GCCS environment.

2. Cancellation. None.

3. Applicability. This instruction applies to CINCs, Services, and Agencies (C/S/A), the Joint Staff, and others who use the GCCS. It is derived from the authority contained in OSD and CJCS direction in references a, b, and c.

4. Policy

a. For the purposes of this instruction, GCCS CM is the application of a disciplined process where changes to the GCCS and its documentation can be recommended, controlled, and implemented without detriment to the GCCS operational environment. The GCCS operational environment includes automatic data processing (ADP) hardware and software, communications hardware and software, and applicable portions of the Defense Information Systems Network (DISN).

b. New requirements are addressed in accordance with applicable OSD direction and reference c. The CM process accepts validated requirements (references b and c) as input to the evolutionary build. New requirements that are identified as a needed product of the operational

baseline and not part of an evolutionary build will be passed to the Joint Staff J-33 (Command Systems Operations Division (CSOD)) for consideration for inclusion into the operational baseline.

c. New GCCS functional requirements and proposals for migration system candidates will be submitted to the Joint Staff (J-33/CSOD). Problem reports (PR) and change requests (CR) will be sent via the GCCS Site Coordinator (GSC) and the Service Help Desks (if applicable) to the GCCS Management Center (GMC) Help Desk for cataloging and insertion into the GCCS CM process. The Joint Staff, C/S/As, and the Defense Information Systems Agency (DISA) will be responsible for appropriate follow-on action as defined in this policy.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A.

7. Summary of Changes. None.

8. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

Enclosures:
A – Responsibilities
B – GCCS CM Structure
C – GCCS CM Activities
D – GCCS CM Process
E – References
Glossary

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	Copies
Secretary of State	2
Secretary of Defense	10
Director of Central Intelligence	20

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for CJCSI 6722.01. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 2	O	C-1 thru C-4	O
i thru vi	O	D-1 thru D-10	O
A-1 thru A-10	O	E-1 thru E-2	O
B-1 thru B-8	O	GL-1 thru GL-17	O
B-A-1 thru B-A-2	O		

(INTENTIONALLY BLANK)

RECORD OF CHANGES

Change No.	Date of Change	Date Entered	Name of Person Entering Change

(INTENTIONALLY BLANK)

ENCLOSURE A

RESPONSIBILITIES

1. Joint Staff. The Chairman of the Joint Chiefs of Staff is responsible for policy guidance and oversight of Global Command and Control (GCC). The Joint Staff J-3 and J-6 are responsible for operational and technical oversight for GCCS and report to the GCCS General/Flag Officer Advisory Board as defined in reference b. The Joint Staff J-3 and J-6 relationships are depicted in Figure A-1 and defined in the following paragraphs.

JOINT STAFF GCCS OVERSIGHT ORGANIZATIONS

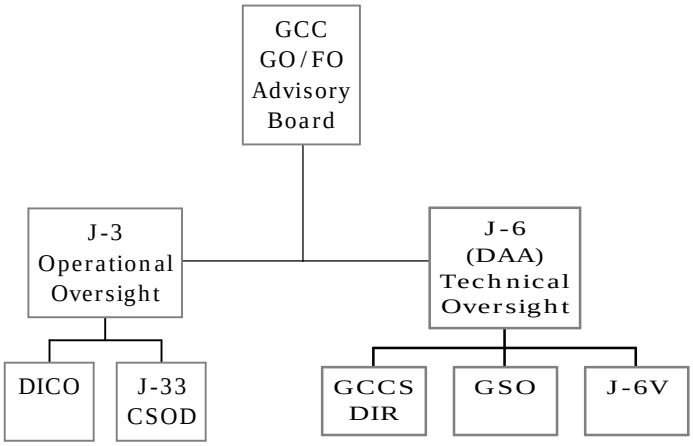

Figure A-1

a. Director for Operations, Joint Staff (J-3). As directed in reference b, the Joint Staff J-3 is the office of primary responsibility (OPR) for GCC. Proposed changes that will require a new evolutionary build or a new baseline will be reviewed and approved/disapproved by the J-3 at the GCC General/Flag Officer Advisory Board. The OPR is assisted by, in descending order, a GCC General/Flag Officer Advisory Board, a planner level GCCS Review Board, the C4 Systems Integration Working Group (SIWG), and functional area working groups.

(1) Data Information Coordination Office (DICO). The Joint Staff (J-3) will designate a DICO to provide operational direction and guidance for the GCCS. The J-3 DICO will be the primary focal point for any issue that may impact the operations of the GCCS. The J-3 DICO will have the authority to authorize extended system outages, priority of repairs, and other activities deemed critical to the operations of the GCCS.

(2) Joint Staff (J-33/Command Systems Operation Division (CSOD)). The Joint Staff J-33/CSOD is the OPR for the management oversight of new functional requirements and proposals for migration of systems to GCCS, as specified in reference c. The J-33/CSOD provides the focal point for ensuring a responsive front end process exists to identify, validate, integrate, and prioritize functional requirements.

b. Director for Command, Control, Communications, and Computer Systems (C4), Joint Staff (J-6). As directed in reference b, the Joint Staff J-6 has technical oversight of GCCS. The J-6 will work closely with the J-3 and DISA to ensure smooth execution of this policy.

(1) GCCS Director (DIR). The J-6 will designate a planner-level (O-6) GCCS DIR to be the focal point for all aspects of GCCS operations related to system and network configuration, fault, performance, and security management. This responsibility includes testing, evaluation, and implementation of the GCCS. It also includes responsibility for continuing coordination with OPRs for systems, such as Global Combat Support System (GCSS) and Joint Deployable Intelligence Support System (JDISS), which need to be closely linked to GCCS efforts, in order to facilitate interoperability and eventual integration and merger of those systems. The GCCS DIR will provide technical solutions to the DICO for an operational decision on global GCCS problems and/or for recommended changes. The J-3 DICO will then forward recommended changes to the GCCS Review Board for final approval.

(2) GCCS Designated Approving Authority (DAA). The J-6 is the DAA for all GCCS security matters. The DAA is responsible for approving security policies, providing security guidance, and taking whatever actions are necessary to ensure the integrity

and security of the GCCS operations. Responsibilities and duties for the GCCS DAA are outlined in reference d.

(3) GCCS Security Officer (GSO). The J-6 will designate a GSO. The GSO is responsible for the day-to-day security operations of the GCCS. As such, all Site GCCS Information System Security Officers (Site GCCS ISSOs) will adhere to the guidance published by the GSO. The GSO is responsible for providing security information and recommendations to the Joint Staff DAA for matters involving the GCCS. Responsibilities and duties for the GSO are outlined in references d and e.

(4) Joint Staff (J-6V). The J-6V has CM as one of its delegated technical oversight roles as defined in references a, b, and c. J-6V will co-chair the GCCS Configuration Control Board (CCB) as defined in Enclosure B. J-6V and the J-33/CSOD will review and approve/disapprove GCCS CCB recommended outages to apply modifications to the GCCS operational environment.

2. DISA. The Director of DISA is responsible for all daily CM activities, as outlined in this instruction, as well as network management and other processes that directly impact GCCS configuration. Along with Joint Staff J-6, DISA has the responsibility for continuing coordination with the OPRs for systems, such as GCSS and JDISS, which need to be closely linked to GCCS efforts, in order to facilitate interoperability and eventual integration and merger of those systems. DISA organizations responsible for CM are depicted in Figure A-2 and collectively perform the following tasks:

DISA CM ORGANIZATIONAL RELATIONSHIPS

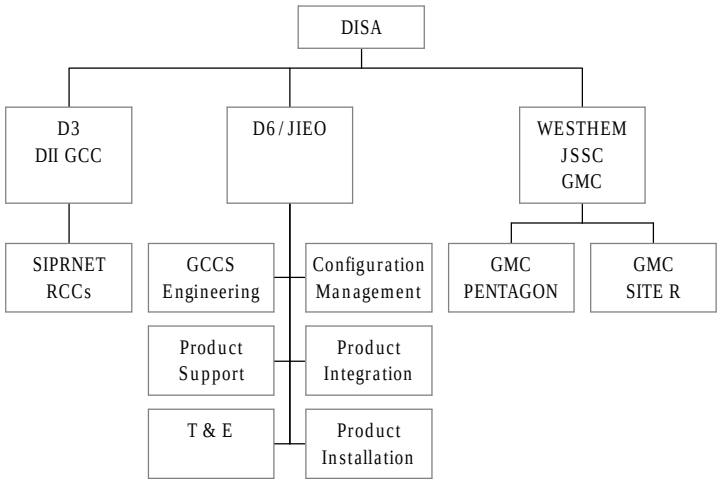

Figure A-2

a. Co-chair the GCCS Configuration Control Board (CCB) as defined in Enclosure B.

b. Coordinate and integrate activities of all DISA organizations working GCCS CM issues as defined in Enclosure B.

c. Coordinate with C/S/As to receive, test, evaluate, and approve/disapprove proposed mission unique and site unique configuration items (CIs) that may impact the GCCS operational environment. This coordination will occur prior to any mission unique or site unique CIs being installed.

d. Integrate C/S/A CM efforts with DISA efforts to optimize efficiency and eliminate redundant and/or contradictory efforts.

e. Monitor GCCS sites to ensure that baseline configurations are maintained and pertinent functional, performance, and physical interfaces between GCCS components and software segments are adequately documented.

f. Coordinate the efforts of the individual GCCS CCBs as outlined in Enclosure B to define GCCS CIs that will be required to be baselined

and determine the documentation that must support all CIs. C/S/A GCCS sites must cooperate in this effort to ensure adherence.

g. Ensure that GCCS CIs are placed under configuration control when the CI is identified.

h. Ensure that change requests or evolutionary builds are processed and evaluated in a timely manner.

i. Ensure that cost, schedule, and performance aspects of change requests, problem reports, and engineering change proposals are known at the time of their consideration by the respective GCCS CCBs.

j. Ensure that DISA maintained specifications, documentation, data, and related baseline information are adequate.

k. Ensure that adequate user, system, and other documentation are created, tested, and maintained for DISA-controlled CIs.

l. Review C/S/A documentation for sufficiency, accuracy, and currency. Provide the C4 SIWG reports of any C/S/A that fails to provide adequate documentation.

m. Lead and/or coordinate all CM audit processes for GCCS.

n. Ensure that GCCS data standardization efforts are timely and conform to applicable DOD standards.

o. Ensure that the system security posture, as defined in references d and e, is neither compromised nor degraded with the application of any change.

p. Oversee all segment releases to the GCCS baseline and control all automatic upgrades to segments in the baseline (to include C/S/A supplied segments that contain automatic update capability).

3. GCCS Sites. A GCCS Site is defined as *all* physical locations where GCCS equipment is installed (e.g., workstations, servers, communications devices). A GCCS Site(s) Coordinator (GSC) may coordinate the activities at more than one GCCS Site (i.e., more than

one physical location). GCCS positions are depicted in Figure A-3. The "*" indicates **mandatory** positions.

GCCS POSITIONS

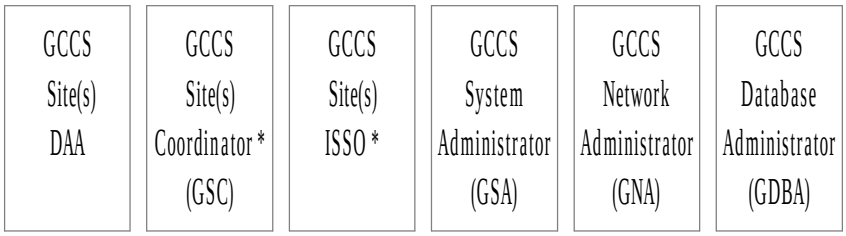

Figure A-3

a. GCCS Site(s) Coordinator (GSC). (**Mandatory Position)** The GSC is responsible for coordinating all system and network support activities within the GCCS site(s). The individual filling this role will be the primary focal point for coordinating with the Service Help Desk (if applicable), the GMC Help Desk, and other GCCS organizations. One of the major duties of this position will be to direct activities during and following an emergency condition to minimize the loss of GCCS mission capabilities at the site. The GSC is also responsible for coordinating with DISA and providing proposed mission unique and site unique CIs for testing and evaluation prior to installation. For large organizations, the site commander or DAA may want to appoint additional personnel in this function. They will be referred to as an Assistant GCCS Site(s) Coordinator (AGSC). Since the GSC is a **mandatory** position, this person should be able to perform the duties of the following positions (with the exception of the GCCS Site(s) ISSO) if manpower constraints prevent additional staffing.

b. GCCS Network Administrator (GNA). The GNA is responsible for the day-to-day operation of the GCCS local area network (LAN); the communications devices (premise router, communications server, and intelligent hubs); and related GCCS equipment. Duties include, but are not limited to:

(1) Operate the LAN.

(2) Maintain the LAN.

(3) Add and remove communications hardware and software.

(4) Maintain the AUTODIN/DMS (future) interface.

(5) Identify and be capable of installing each LAN component.

(6) Maintain LAN system interfaces.

(7) Troubleshoot network and communications problems.

(8) Provide expertise in protocol services.

c. GCCS System Administrator (GSA). The GSA is responsible for a variety of duties with the major focus being on maintaining the GCCS workstation, providing local user support, and troubleshooting site problems associated with the GCCS applications. A thorough understanding of the Defense Information Infrastructure (DII) Common Operating Environment (COE) architecture will be instrumental in accomplishing the duties of this position. Duties include, but are not limited to:

(1) Direct activities during and following an emergency condition to minimize the loss of GCCS mission capabilities at the site.

(2) Administer access permission lists based on ISSO guidance.

(3) Maintain the Executive Manager permissions program.

(4) Add and remove hardware and software.

(5) Perform system startups, backups, and upgrades.

(6) Generate periodic summaries of system performance and utilization.

(7) Routinely backup data and audit files.

(8) Coordinate the management of GCCS User IDs with the ISSO.

(9) Diagnose system problems and report them to the GSC, the C/S/A Help Desk (if applicable), and the GMC Help Desk.

(10) Monitor total system performance to ensure optimal performance.

(11) Reconfigure GCCS to regain processing capabilities for nonroutine equipment malfunctions.

(12) Assist users in determining the cause of failures.

d. GCCS Database Administrator (GDBA). The GDBA is responsible for the day-to-day operations of the databases located at the GCCS site. This may include the primary database server (Sun Sparc 1000 or Sparc 2000) running the Oracle Relational Database Management System (RDBMS), or the Executive Manager application using the Sybase RDBMS, or the Automated Message Handling System (AMHS) server application using the Verity Topic RDBMS. Duties include, but are not limited to:

(1) Coordinate incremental/partial backups of the databases with the GSC and the GMC-Pentagon.

(2) Generate periodic summaries of database performance and utilization.

(3) Coordinate database modifications with other site personnel.

(4) Monitor all database applications for proper performance.

(5) Manage disk/tape storage.

(6) Diagnose database and database-to-application problems and resolve or report to the GSC.

e. GCCS Site(s) DAA. The GCCS Site(s) DAA is responsible for local security policies and guidance to ensure the integrity and security of the GCCS operations are maintained. Receives direction and guidance from the Joint Staff (J-6) GCCS DAA or his designated representative. The GCCS Site(s) DAA is responsible for accrediting GCCS at the site(s).

f. GCCS Site(s) Information Systems Security Officer (ISSO). **(Mandatory Position)** The GCCS Site(s) ISSO is responsible for ensuring the integrity and security of the local GCCS system and network. The GCCS Site(s) ISSO is responsible for providing security information to the site(s) GCCS DAAs. The duties of the GCCS Site(s) ISSO are identified in reference d.

(INTENTIONALLY BLANK)

ENCLOSURE B

GCCS CM STRUCTURE

1. Global Command and Control (GCC) Management Structure. The GCC Management Structure is defined in reference b. Primary functions of the GCC Management Structure are listed as follows:

a. GCCS Review Board. The GCCS Review Board is chaired by the Vice Director for Command, Control, Communications, and Computers, (VJ-6). It is the primary body charged with consolidating, and validating changes to the GCCS, in accordance with references a through c. It also reviews and approves charters for the Functional Area Working Groups and the C4 SIWG. All new requirements that have been validated by the Joint Staff J-3 and have been technically validated by DISA will be given to the GCCS Review Board to prioritize. These prioritized requirements will then be prepared for the GCC General/Flag Officer Advisory Board for approval/disapproval. The GCCS Review Board, as specified in this instruction, will also review recommendations and resolve issues forwarded by the C4 SIWG and the GCCS CCB. As defined in reference b, it will forward issues that cannot be resolved (i.e. funding issues, new baselines, unresolved issues from other boards) to the GCC General/Flag Officer Advisory Board.

b. C4 Systems Integration Working Group (SIWG). The C4 SIWG, which is chaired by a representative from the Joint Staff J-6, has as one of its functions the oversight of CM for the various working groups, as specified in reference b. The C4 SIWG will coordinate with the GCCS CCB to verify the correctness of all recommended modifications to the GCCS operational environment prior to implementation. In coordination with the J-33/CSOD, the C4 SIWG coordinates on GCCS CCB recommended outages to apply upgrades. Issues the C4 SIWG cannot resolve will be forwarded to the GCCS Review Board. The C4 SIWG will coordinate with DISA on the performance of technical and programmatic audits and reviews and will provide recommendations as necessary to the GCCS Review Board.

2. GCCS Collaborative CM Environment. CM is a management discipline that applies technical and administrative direction to the development, production, and support life cycle of a CI. This discipline is applicable to hardware, software, networking infrastructure, processed materials,

services, and related technical documentation. CM is an integral part of life-cycle management. The main objective of CM is to ensure the integrity of the product by documenting and providing full visibility of the product's present configuration and the status of achievement of its functional and physical requirements. Because of the inherent nature of distributed processing and communications environments, CM becomes a difficult task and generally requires the efforts of many organizations to accomplish CM objectives. The GCCS operational environment is a distributed processing and communications environment. Because of the number of diverse organizations involved in GCCS CM, a collaborative CM environment is established to manage GCCS CM. This collaborative CM environment is depicted in Figure B-1 and responsible organizations are identified in the following paragraphs.

GCCS COLLABORATIVE CM ENVIRONMENT

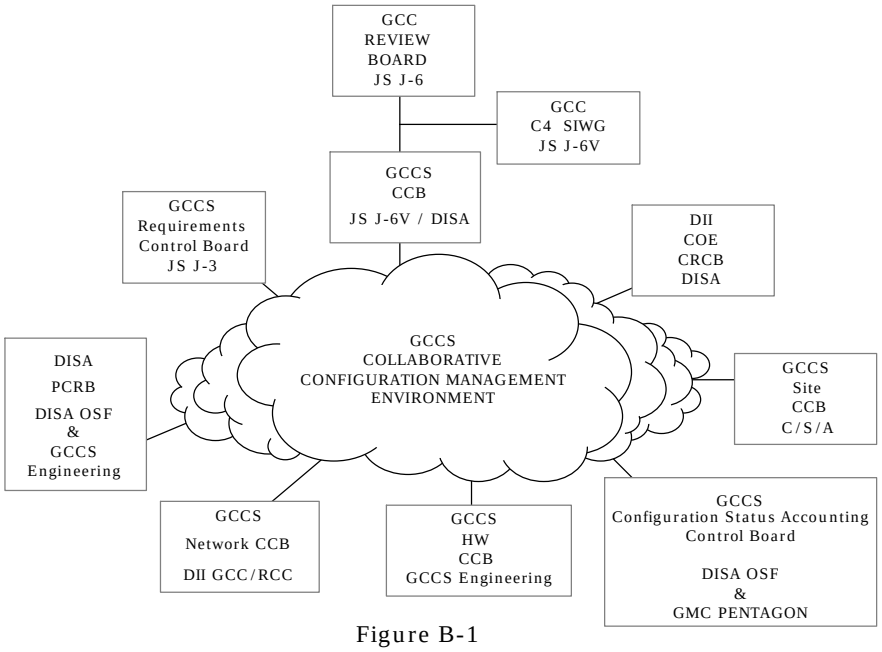

Figure B-1

a. GCCS Configuration Control Board (CCB)

(1) Scope. The GCCS CCB is concerned with all GCCS CM issues. Primary functions are to create an evolutionary build list, to resolve issues, to review technical aspects of the various baselines, to ensure that GCCS is developed and maintained according to specifications, to review overall program management issues, to review recommended changes to joint mission area applications,

and to ensure a consistent GCCS change control process, and to ensure that validated requirements are correctly reflected and prioritized in the DISA work plan. The GCCS CCB will approve actions to complete all change requests and will forward for validation to the Joint Staff (J-33/CSOD) all PRs/CRs that demand an evolutionary build.

(2) Chair. The GCCS CCB will be co-chaired by the Joint Staff J-6V and DISA and will be under the functional and technical oversight of the GCCS Review Board.

(3) Membership

(a) Regular Members. Regular CCB members are designated representatives from C/S/As, Joint Staff (J-2, J-3, J-4, J-5, J-6, J-7, J-8), and DISA. Functional Area Working Group chairs, the C4 SIWG chair, or their representatives will be invited to sessions with agendas applicable to that working group's area of responsibility. Others that may be included as appropriate are: United States Coast Guard, National Imagery and Mapping Agency, Defense Logistics Agency, National Security Agency, and OSD (C3I).

(b) Advisory Attendees. The co-chairs may invite advisory members.

(4) Meeting Frequency. The co-chairs will determine when to hold meetings. Announcement of meetings will be made as far in advance as possible to permit C/S/A representatives to attend.

(5) Charter. The GCCS CCB charter requirements are specified in Appendix A to this enclosure.

b. GCCS Requirements Control Board

(1) Scope. The GCCS Requirements Control Board will provide oversight of the submission process for GCCS joint functional requirements. All C/S/As and GCCS working groups may input requirements for GCCS. The appointed GCCS approving authority for each organization must input the requirement using the Global Command and Control Requirements Database (GRiD). The submission needs endorsement at the O-6 level (GCCS Review Board Member or working group chair) or above, to the Joint Staff,

J-33/CSOD.

(2) Chair. The Joint Staff J-33/CSOD.

(3) Membership. As directed by the chair.

(4) Meeting Frequency. As directed by the chair.

(5) Charter. N/A. Guiding principles are contained in reference c.

c. DII COE Configuration Review and Control Board (CRCB)

(1) Scope. A DISA established CRCB to act as a forum for the approval of proposed changes and improvements to common products, approval of development software build plans, and oversight of the software development process for the DII COE. The CRCB will manage changes to common computer software configuration items (CSCI) used in subscriber systems. Common CSCIs include the common operating environment (COE), the associated engineering standards and conventions, and other software products selected by the CRCB for joint configuration management.

(2) Chair. As directed by DISA.

(3) Membership. As directed by the CRCB charter.

(4) Meeting Frequency. As directed by the chair.

(5) Charter. The DII COE CRCB is chartered in accordance with OSD (C3I) and DISA guidance.

d. GCCS Hardware (HW) CCB

(1) Scope. The DISA GCCS Engineering Office will be responsible for ensuring that the hardware platforms implemented will adequately handle the processing and communications workload for each workstation. This requirement includes testing and evaluation of proposed additions to the joint software that is planned for each GCCS site. The GCCS HW CCB coordinates all hardware releases with the GCCS CCB.

(2) Chair. DISA GCCS Engineer.

(3) Membership. As directed by the chair. C/S/As may participate when issues pertain to them. DISA will place the upcoming agenda on SIPRNET so any C/S/A can determine if they should participate. DISA will provide adequate advance notice to permit CINC representatives to attend.

(4) Meeting Frequency. As directed by the chair.

(5) Charter. As directed by DISA.

e. GCCS Network CCB--Scope. The top level DII control center is referred to as the Global Control Center (GCC) that is operated by the DISA C4I Network Systems Management Division (D31). The GCC provides management oversight for the networks of the DII for which DISA has network management responsibility. These networks include the SIPRNET, GGCS' backbone communications infrastructure. The second layer is comprised of the regional control centers (RCCs). The RCCs are responsible for the day-to-day operations of the networks under their immediate control. They are geographically oriented with several centers dispersed across the United States, a center located at the DISA European facilities to cover Europe, and another located at the DISA Pacific facilities to cover the Pacific assets. The RCCs are responsible for the DISA assets within their areas and operate as peers to each other. The RCCs responsible for various portions of the SIPRNET are also responsible for the health of the DISN routers installed on those networks. The RCCs and the GCC are responsible for DISA assets only. They do not control any assets owned by the individual C/S/As connected to the networks or WANs. The GCCS premise routers are included in the list of equipment that the GCC and the RCCs do not manage. The GCCS community is responsible for managing these assets. This is where the third layer of the hierarchy model comes in to play. These management centers, or DII control centers, are referred to as local control centers (LCCs) and they belong to the individual subscriber communities. In the case of the GCCS, the community must establish LCCs to manage the GCCS assets. The DISN RCCs will coordinate with the GMC-Pentagon on all efforts to detect, isolate, and correct problems associated with the GCCS. The GCCS Network CCB coordinates all Network CI releases with the GCCS CCB.

(1) Chair. DISA D3 designate.

(2) Membership. As directed by the chair.

(3) Meeting Frequency. As directed by the chair.

(4) Charter. As directed by DISA.

f. GCCS Configuration Status Accounting (CSA) Control Board

(1) Scope. DISA OSF CM Division is responsible for the implementation of CIs and CSCIs, both prior to the operational implementation and throughout the life cycle of the CIs and CSCIs. All fielded GCCS CIs and CSCIs, including baselines and proposed changes, will be tracked by the GMC Pentagon.

(2) Chair. DISA.

(3) Membership. As directed by DISA, but includes GMC Pentagon and OSF CM Division.

(4) Meeting Frequency. As directed by DISA.

(5) Charter. DISA Standard Operating Procedures (SOPs).

g. GCCS Site CCB

(1) Scope

a. It is recognized that C/S/A GSCs may have an internal CM process, which encompasses C/S/A specific configurables. This instruction does not address the CM process of individual C/S/As. The GCCS CCB will control submitted changes by defining and enforcing adherence to the standards and integration requirements.

b. GSCs are responsible for coordinating with DISA and providing proposed mission unique and site unique CIs for testing and evaluation prior to installation.

c. C/S/As will ensure that modifications to applications do not impact any GCCS functionality and will be responsible for immediate corrective action when impact occurs.

d. Each GSC is responsible for site hardware/software configurations, inventories, and site unique applications residing on GCCS. The GSC documents and monitors the site's configuration and reports all relevant configuration changes to the GMC Pentagon.

e. Each GCCS site will have a process to monitor and audit its GCCS hardware (this includes the hardware description, connections, locations, types, installation diagrams, clients/servers, etc.) and the software (software descriptions, versions, and documentation for applications, databases).

f. It is anticipated that most issues can be resolved by the GCCS CCB. If not, the issue will be referred to the C4 SIWG and GCCS Review Board. The GCCS Review Board will forward all issues it cannot resolve to the GCC General/Flag Officer Advisory Board.

(2) Chair. As directed by the C/S/As.

(3) Membership. As directed by the C/S/As.

(4) Meeting Frequency. As directed by the C/S/As.

(5) Charter. As directed by the C/S/As.

h. DISA Problem/Change Review Board (PCRB)

(1) Scope. The main task of the DISA PCRB is the evaluation of problem reports (PRs), change requests (CRs), and the implementation of corrective action and/or modifications. GCCS Functional Working Groups will assist the PCRB with PR/ECP/CR priority establishment as defined in paragraphs D2b and D3 of this instruction. Recommendations for priority changes will be forwarded to the GCCS CCB for a decision. The PCRB will provide user feedback to the C/S/As, and Joint Staff, concerning the prioritizing of PRs/CRs. DISA will maintain, on line, the current status of all open GCCS PRs/CRs as they progress within the change management process. Any unresolved issues, or issues

which extend beyond problem fixes, will be forwarded to the GCCS CCB for resolution. If a PR or CR is determined to be a new requirement to the baseline, then DISA will forward it to the Joint Staff (J-33 CSOD) for initial processing.

(2) Co-chair. DISA OSF CM Division and GCCS Engineering.

(3) Membership. The PCRB will consist of members from the Joint Staff (J-3 and J-6), GCCS Systems Engineering, GMC, and others designated by DISA. C/S/As may participate when issues pertain to them. DISA will place the upcoming PCRB agenda on SIPRNET so any C/S/A can determine if they should participate. DISA will provide adequate advance notice to permit C/S/A representatives to attend.

(4) Meeting Frequency. As directed by DISA.

(5) Charter. The PCRB charter requirements are specified in Appendix A to this enclosure.

APPENDIX TO ENCLOSURE B

CCB/PCRB CHARTERS AND MINUTES

1. Charters. The GCCS Review Board will approve charters for the GCCS CCBs and PCRB. Each charter will contain the following:

a. Purpose and major objectives of the board.

b. Identification and responsibilities of the chair.

c. Membership responsibilities.

d. Advisory membership and responsibilities if applicable.

e. Relationships and responsibilities of the board to external organizations, to the GCC management structure, and to other boards with CM responsibilities.

f. Frequency of meetings, procedures for timely notification of attendees (including CINC representatives), and distribution list for minutes.

g. Procedures for modifying the charter.

2. Minutes and Dissemination of Information. A recorder will create the agenda, track action items, and record, publish and distribute minutes for each CCB/PCRB. Minutes will be available on line via SIPRNET. The DISA PCRB will provide monthly summaries to the GCCS CCB.

(INTENTIONALLY BLANK)

ENCLOSURE C

GCCS CM ACTIVITIES

1. Configuration Identification

a. Overview. Configuration identification includes selection of configuration items (CIs), determination of the types of configuration documentation required for each, the issue of numbers or identifiers affixed to each CI and the technical documentation describing its configuration (to include internal and external interfaces), the release of associated documentation, and the establishment of configuration baselines. All CIs for GCCS will be controlled following the guidelines in references f, g, h, i, j, and o.

b. Designation of CIs. Items to be designated as CIs include the following:

(1) All aggregations of hardware, software, and firmware that satisfy GCCS requirements. CIs can be logically designed, implemented, tested, and maintained as separate entities.

(2) Documents that describe technical aspects of the CIs such as functional specifications, design specifications, application programming interfaces (APIs), and operational specifications.

(3) Documents that describe CI management, configuration management and quality assurance processes, test plans, test reports, applicable minutes of CCBs, and user manuals.

c. Tasks. The purpose of configuration identification is to incrementally establish and maintain a definitive basis for configuration control and status accounting for a CI throughout its life cycle. To accomplish this DISA, C/S/As, GSCs, and the Joint Staff will:

(1) Develop configuration documentation to define the configuration baselines for each CI, its components, and its interfaces.

(2) Establish a release system for configuration documentation.

(3) Align system requirements with CIs.

(4) Define and establish a quality assurance process (to include standards) for testing, documentation, product release, and providing CI information to Configuration Status Accounting personnel.

d. GCCS Software Applications Relationships. Understanding GCCS software application relationships provides the GCCS CM community with a logical method of controlling changes for the GCCS operational environment. Since GCCS is migrating to the DII COE, these relationships are defined in DII COE terms. A DII COE Taxonomy is depicted in Figure C-1.

DII COE TAXONOMY

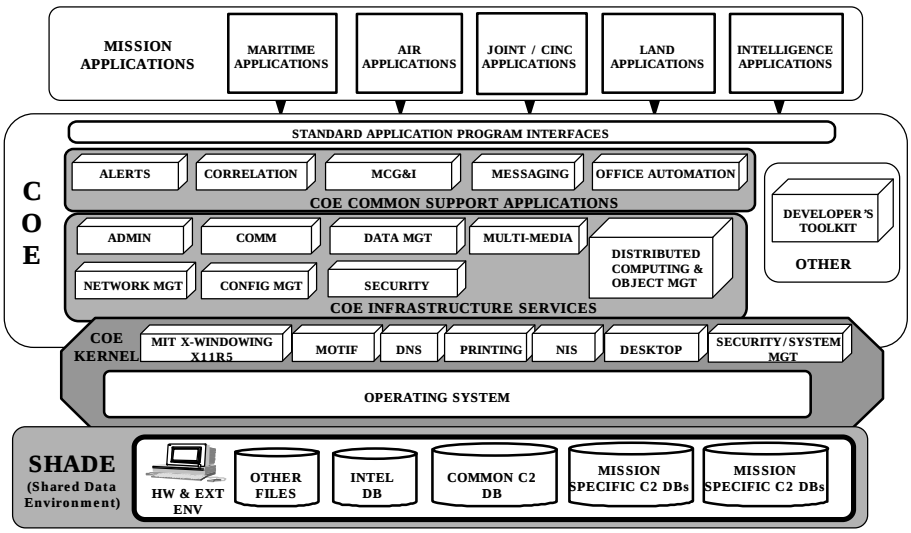

Figure C-1

The DII COE software illustrates the relationships between the Kernel, Infrastructure Services, and Common Support Applications. Figure C-1 also illustrates a conceptual view of how joint mission applications, C/S/A mission unique applications, and site unique applications interface with the DII COE through Application Program Interfaces (APIs). APIs provide joint mission applications, C/S/A mission unique applications, and site unique applications access to the components of the COE. The COE and joint mission applications

represent joint requirements. GCCS SW application examples are depicted in Figure C-2.

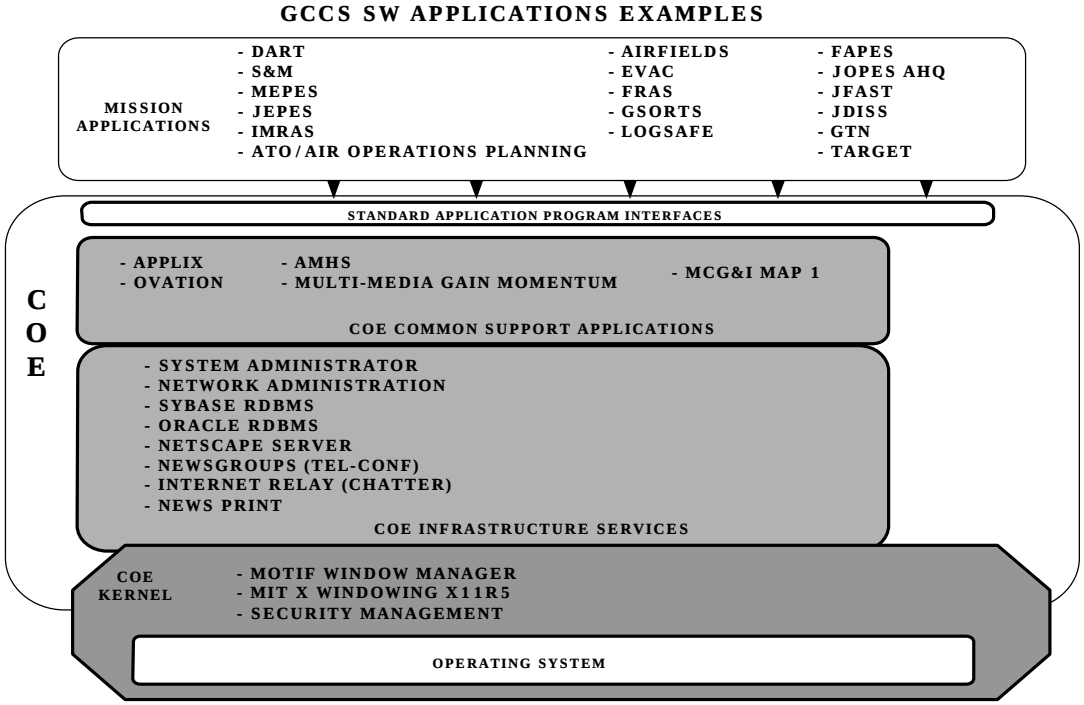

Figure C-2

C/S/A mission unique and site unique applications should not impact the functionality or performance of GCCS. They reside in GCCS, but are not part of the joint mission requirements of GCCS. CIs in the COE are under control of the DII COE CRCB, subject to coordination with and approval by the GCCS CCB, SIWG, and GCCS Review Board for issues involving CIs comprising embedded user functionality. CIs for mission unique and site unique applications are under combined control of the GCCS PCRB, CCB, GSC, and the GCCS site CCBs.

2. Configuration Control. Configuration control is the systematic proposal, justification, evaluation, coordination, and approval/disapproval of proposed changes, and the implementation of all approved changes. The goals of GCCS configuration control are:

a. To ensure effective control and oversight of all CIs and their approved configuration documentation.

b. To ensure regulation of the flow of proposed changes, documentation of the complete impact of the proposed changes, and release of only those changes that have been approved.

c. To ensure that changes, to include C/S/A mission unique and site unique changes, do not adversely impact GCCS.

d. To ensure that changes are cost effective, timely, and meet the users needs.

e. To provide an open change control forum where parties can discuss issues.

f. To manage the engineering change proposal (ECP) and other change processes and oversee the implementation of approved changes.

g. To ensure implementation of all approved changes.

h. To ensure integrated logistics support (ILS) is provided.

3. Configuration Status Accounting (CSA). CSA is the recording and reporting of information needed to manage CIs effectively. CSA occurs throughout the life cycle of the CI or the Computer Software Configuration Item (CSCI). The process begins with the initial registration of the CSCI by the segment developer or with the purchase of a hardware CI. Responsibility for CSA during this portion of the life cycle is primarily with the DISA OSF CM Division. Once the CI or CSCI becomes part of the operational system, through the shipment of a hardware CI to a GCCS Site or inclusion of a CSCI as part of an official release, CSA becomes primarily the responsibility of the GMC Pentagon.

4. Configuration Audits (CA). In the rapid prototyping environment, functional and physical configuration audits are not required. C/S/As who sponsor individual applications may conduct audits, as needed, prior to the delivery of the application to the DISA OSF.

ENCLOSURE D

GCCS CM PROCESS

Specific details of the GCCS CM process are discussed in reference o.

1. New Functional Requirements. C/S/As and GCCS working groups may input requirements for GCCS. The appointed C/S/A GCCS approving authority will input the requirement using the GCCS Requirements Database (GRiD) as directed in reference c. The Joint Staff J-33/CSOD, in coordination with the C4 SIWG, will track and further disseminate requirements to Functional Area Working Groups for validation and recommendation as to the type of GCCS application that will satisfy the requirement (e.g., joint mission area application, DII COE segment). DISA is responsible for the technical evaluation after completion of the functional validation process.

   a. Functional Tracking. The Joint Staff J-33/CSOD and the Functional Area Working Groups will track the status of functional requirements in GRiD.

   b. Technical Tracking. DISA will maintain a database to track proposed, approved, and implemented technical solutions that satisfy functional requirements. The Joint Staff, CINCs, Services, and other authorized users will have access to the database to determine the status of these requirements.

2. Problem Reports (PR)

   a. A PR initiates the process of getting a malfunctioning CI fixed. PRs are coordinated through GCCS Site Coordinators (GSC). Every effort will be made to resolve the problem at the GCCS Site. GCCS Sites unable to resolve the problem will forward the request for problem resolution to the Service Help Desk (if applicable). If the problem cannot be resolved by the Service Help Desk, the PR will be forwarded to the GMC Help Desk. Generally, Service Help Desks (if applicable) can resolve problems and prevent the GMC Help Desk from being flooded with GCCS problems that can be resolved at lower levels.

b. Once the GMC Help Desk is involved, it will forward unresolved PRs and their status to the GCCS PCRB. The GCCS PCRB will evaluate the technical feasibility and provide cost estimates, technical recommendations, and scheduling implications to the appropriate Functional Working Groups. These Functional Working Groups, serving as executive agents for the GCCS Review Board, will prioritize the PRs and forward the prioritized requirements to the GCCS PCRB for appropriate action. Unresolved PCRB issues will be forwarded to the GCCS CCB and/or the GCCS Review Board for a decision. Functional Working Groups must ensure that their prioritization decisions do not negatively impact other functional areas, the GCCS system functionality, security, or the DII COE.

c. All PRs will be recorded, even if solved immediately. Each C/S/A Help Desk (if applicable) and GSC will maintain a database of PRs. If an answer or solution is not possible immediately, the GMC Help Desk will perform a triage function and route the issue/request to a specialist organization for action. The GMC Help Desk will assist in determining what the proper categorization of the unresolved trouble call should be (i.e., PR, ECP, new functional requirement). All PRs submitted to the GCCS PCRB will be tracked in the CM system and made available to approved CM users via SIPRNET.

d. GSCs are responsible for tracking and resolution of PRs for mission unique and site unique CIs.

e. Joint Universal Lessons Learned (JULLS) are submissions of lessons learned from any source (e.g., C/S/A, the Joint Staff), according to reference k. They are usually a result of an exercise and generally identify problems that have occurred. JULLS that require resolution can be of a functional, administrative, or technical nature. The Joint Staff's Remedial Action Projects (RAP) Steering Group is responsible for the oversight of JULLS and their resolution. JULLS that are technical and pertain to GCCS will be given to the GMC Help Desk and categorized as PRs. They will then be tracked by DISA as a PR.

f. PRs that have been submitted may be converted to ECPs or new requirements proposals after they are reviewed by the DISA PCRB. If converted, the PR status on the DISA *Homepage* will be updated to reflect the change. PRs converted to ECPs or new requirements proposals are tracked in the CM system under the new category.

3. Engineering Change Proposals (ECP)/Change Requests (CR). ECPs, commonly referred to as CRs, will be submitted through the GSC, via the Service Help desk (If applicable), to the GMC Help Desk. The GMC Help Desk will record all ECPs for tracking and will forward to the PCRB for formal action. The PCRB will evaluate the technical feasibility and provide cost estimates, technical recommendations, and scheduling implications to the appropriate Functional Working Groups. These Functional Working Groups, serving as executive agents for the GCCS Review Board, will prioritize the ECPs and forward the prioritized requirements to the GCCS PCRB for appropriate action. Unresolved PCRB issues will be forwarded to the GCCS CCB and/or the GCCS Review Board for a decision. Functional Working Groups must ensure that their prioritization decisions do not negatively impact other functional areas, the GCCS system functionality, security, or the DII COE.

a. Analysis of GCCS ECPs/CRs. DISA will monitor the full analysis of the ECP, to include costing and system impact.

(1) Mislabeled New Requirements. If analysis determines that a ECP is actually a new requirement, DISA will forward the ECP to the Joint Staff (J-33/CSOD). DISA will inform the submittor that the ECP is a new requirement and has been forwarded to the Joint Staff (J-33/CSOD) and the submittor must follow the directions as outline in reference c for new requirements. The Joint Staff (J-33 CSOD) will log and track the new requirement in accordance with Enclosure D, paragraph 1 above.

(2) Mission Unique and Site Unique ECPs/CRs. C/S/As will indicate that the ECP/CR is for a mission unique or site unique CI. GSCs will coordinate with DISA and provide proposed mission unique and site unique CIs for testing and evaluation prior to installation. C/S/As must demonstrate that the proposed CI will not negatively impact GCCS functionality, security, or the DII COE. The determination of impact will include security aspects that may harm GCCS or the SIPRNET. All GCCS connectivity must be analyzed to ensure a link is not vulnerable to intrusion attempts. If a CI is determined to impact GCCS or the DII COE, then the C/S/A will resolve the issue to DISA's satisfaction. C/S/As who do not agree with DISA findings may submit a waiver in accordance with paragraph 4 below. A memorandum of the problem and the resolution will be sent from the GCCS CCB to the C4 SIWG prior to installation. This will be used for information purposes and will be forwarded to the GCCS Review Board.

b. Logging. All ECPs will be controlled and logged by DISA. The logged ECP will be updated to reflect the status of the ECP to include approved, applied, tested, documented, and integrated.

c. Approval. The implementation of ECPs will be approved by GCC General/Flag Advisory Board with the exception of mission unique and site unique ECPs, which will be approved by the GCCS CCB.

d. Closing ECPs. Closing an ECP requires written concurrence from the submittor or the GCCS Review Board.

e. Classification of ECPs. As per reference l, system maintainers of the system in question will analyze the ECP and classify it as either Class I (emergency, urgent, or routine) or Class II. The classification of the ECP determines the priority order of analysis and implementation of the proposed change.

(1) Class I ECPs. Class I ECPs should be limited to those which offer significant benefit to the government. Normally, such changes correct serious deficiencies; add or modify interface or interoperability requirements; make significant and measurable effectiveness change in the operational environment capabilities or logistics supportability; effect substantial life-cycle costs/savings. An ECP could be a Class I if it would impact one of the following: safety; compatibility or specified interoperability with interfacing CIs or support software; configuration to the extent that retrofit would be required; operation or maintenance manuals for which adequate revision funding is not provided; interchangeability of CIs; sources of CIs or repairable items; skills; manning; training; or human engineering design.

(2) Types of Class I ECPs. The criticality of the need for a technical decision will dictate the priority of a Class I ECP. Target technical decision times are 48 hours for Emergency, 30 calendar days for Urgent, and 90 calendar days for Routine. C/S/A submitting ECPs will consider these targets when assigning a priority to the proposed change.

(a) Class I Emergency ECP (48 hours technical decision response time). An emergency priority will be assigned to a proposed Class I change for one of the following reasons:

1. To effect a change in operational characteristics which, if not completed without delay, may seriously compromise national security.

2. To correct a hazardous situation that may result in fatal or serious injury to personnel or may cause extensive damage or destruction of equipment.

3. To correct a significant system abnormal termination.

(b) Class I Urgent ECP (30 calendar day technical decision response time). An urgent priority will be assigned to a proposed Class I change for one of the following reasons:

1. To effect a change which, if not completed expeditiously, may seriously compromise mission effectiveness of equipment, software, or forces.

2. To correct a potentially hazardous condition that could result in injury to personnel or damage to equipment.

3. To effect a significant net life cycle cost savings to the government, as defined in the contract, through value engineering or through other cost reduction efforts where expedited processing of the change will be a major factor in realizing lower costs.

4. To correct unusable output critical to mission accomplishment.

5. To correct critical CI files that are being degraded.

(c) Class I Routine ECP (90 calendar day technical decision response time). A routine priority will be assigned to a proposed Class I change when emergency or urgent is not applicable.

(3) Class II ECP. A change which impacts none of the Class I factors specified in this instruction is classified as a Class II routine change. Class II ECPs will be incorporated into the next major release not yet in development.

4. Waiver Requests. Waiver requests are requests to modify or deviate from a requirement or specification due to changes in management direction, scheduling, cost, or some other compelling factor. The GCCS CCB will classify waiver requests as critical, major, or minor. A critical waiver requests a departure from a requirement classified as critical or consists of acceptance of a CI that does not conform to safety requirements. A major waiver requests a departure from a requirement classified as major. Also, it could consist of acceptance of a CI involving requirements of health; performance; interchangeability; reliability; survivability; maintainability of the CI or its repair parts; effective use or operation; weight; or appearance (when a factor). A minor waiver requests a departure from a requirement classified as minor, or consists of acceptance of a CI that does not involve any factors listed above for critical or major.

a. Submission. All waiver submissions will be through the GSCs to the GMC Help Desk (except waivers related to new requirements or proposed migration systems).

b. Processing of Requests. The GCCS CCB will review and act on waiver requests. They will forward critical and major waiver requests with recommendations within 15 calendar days of receipt. They will forward minor waiver requests within 30 calendar days. The status of the waivers and their response will be reported to the submittor via SIPRNET. If the submittor does not agree with the response, then they may refer the request to the GCCS Review Board.

5. Change Control

a. Security. All CCB change control processes must adhere to references d and e. All CCBs will include a security representative as an ad hoc member.

b. SIPRNET Operational Control. The DISA Global Control Center (no organizational relationship with GCCS) has operational control of the SIPRNET up to the premise internet protocol (IP) router at the GCCS site. As previously stated in subparagraph B2f, the GCC provides management oversight for the networks of the DII for which DISA has network management responsibility. These networks include the SIPRNET, the backbone communications infrastructure for GCCS. The RCCs responsible for various portions of the SIPRNET are also responsible for the health of the DISN routers installed on those networks. The RCCs and the GCC are responsible for DISA assets

only. They do not control any assets owned by the individual C/S/As connected to the networks or WANs. The GCCS premise routers are included in the list of equipment that the GCC and the RCCs do not manage. It is the responsibility of the GCCS sites or support organizations to manage these assets. GCCS sites will establish LCCs to manage the GCCS assets. The DISN RCCs will coordinate with the GMC Pentagon on all efforts to detect, isolate, and correct problems associated with the GCCS. Current SIPRNET accreditation policies for site local area network service remains in effect, with oversight from the DISA Security Accreditation Working Group.

c. Connections Between GCCS Sites and Other Systems. Connections between GCCS sites and other systems require applicable DAA approval. A MOU must be written which details the scope of intrusion/cross-connection between the systems as it pertains to reference n. The Joint Staff (J-3/J-6) may direct DISA to direct C/S/As to disconnect systems from GCCS interfaces who violate this policy. Any change in the configuration of a connected system requires a review of the connection approval by the DAA.

d. Software (SW) Change Control Levels

(1) Joint Mission Area Application Change Control. Joint mission area applications are considered those that support multiple C/S/As. The following comprise joint mission area applications change control:

(a) Documentation Required from C/S/A. C/S/As will provide all necessary documentation for life cycle support, to include GCCS specific user manuals. C/S/As will provide to the GCCS CCB, hard copy and electronic documentation in a standardized format defined by DISA.

(b) Funding for Documentation. Documentation for C/S/A provided functionality is the responsibility of the C/S/A in accordance with the provisions of a MOU. DISA and the C/S/A will negotiate the terms of funding for documentation during the MOU coordination process or during the C/S/As major segment releases. Any unresolved issues are forwarded to the GCCS CCB and/or the GCCS Review Board for resolution.

(c) Software Certification. C/S/As will certify that all software segments are compliant with the DII COE, security requirements have been met and segments are virus-free.

(d) Approval Authority for Changes. Subject to GCCS Review Board oversight, the GCCS CCB may deny the implementation of any change to joint mission area applications that negatively impacts the cost, schedule, and functionality of GCCS. DISA will maintain an archived copy of the baseline, while the C/S/A GCCS Site CCBs maintaining the CI will retain the original baseline of record.

(2) DII COE. The DII COE supports an open systems environment in accordance with the Department of Defense (DOD) Technical Architecture Framework for Information Management (TAFIM) and the Joint Technical Architecture (JTA). The DII COE includes COTS and GOTS applications and standard APIs that run on multiple hardware platforms. The objective of the DII COE is to provide a common application environment that satisfies the individual needs of many DOD applications. This evolving environment will ensure successful integration of a common set of information processing services that supports individual mission area requirements. The DII COE CRCB will control modifications to the DII COE, with assistance from Joint Staff and the C/S/As.

(a) DII COE Application Categories. Individual DII COE applications belong primarily to one of three general categories:

1. Kernel applications provide basic operating and system services.

2. Infrastructure services support the flow of information throughout the DII network. These services are commonly found on a wide variety of commercial distributed systems and provide such capabilities as database managers and systems administration.

3. Common support applications do not directly support the flow of information throughout the network, but are critical to interoperability. These services include end-user applications such as office automation products and

mission oriented applications ("embedded user functionality") such as track correlators and alert services.

(b) Documentation Required. DII COE developers/maintainers will provide all necessary documentation for life cycle support.

(c) Software Certification. DISA will certify that all software segments are compliant will DII COE requirements, security requirements have been met, and all segments are virus free.

(d) Approval Authority. The DII COE CRCB will approve changes to the DII COE. If proposed changes to the DII COE include GCCS *embedded user functionality,* as defined in this policy, the GCCS CCB and the GCCS Review Board must also approve the changes and verify that the *embedded mission application and/or functionality* is not adversely impacted. DISA will maintain an archived copy of the baseline.

(3) C/S/A Mission Unique and Site Unique Requirements. If a C/S/A has requirements for mission unique or site unique functions that are not joint requirements, they will submit the CIs as an ECP/CR as defined in Enclosure D, paragraph 3 above. These submissions will occur prior to the installation of any CIs. If any C/S/A mission unique or site unique applications evolve into joint requirements, then they may be proposed as migration candidates or components to an evolutionary build.

(a) DII COE Impact. Mission unique and site unique applications must demonstrate the capability to run on the DII COE without impacting other integrated products. Compliance with reference m is mandatory.

(b) Software Certification. C/S/As will certify that all software segments are compliant with the DII COE, security requirements have been met, and segments are virus free.

(c) Approval Authority. DISA will approve/disapprove use of mission unique and site unique software in accordance with paragraph 3a2 above.

(INTENTIONALLY BLANK)

ENCLOSURE E

REFERENCES

a. ASD(C3I) memorandum, 26 June 1995, "Management and Life-Cycle Support for the Global Command and Control System"

b. CJCSI 6721.01 Series, "Global Command and Control Management Structure"

c. "GCCS Mission Area Functional Requirements Evaluation Procedures," Joint Staff (J33/CSOD)

d. CJCSI 6731.01 Series, "GCCS Security Policy"

e. CJCSM 6731.01 Series, "GCCS Security Manual"

f. "Quality Management, Guidelines for Configuration Management," ISO 10007

g. "Configuration Management," Electronic Industries Association, Engineering Department, EIA/IS-649

h. "Integral Life Cycle Processes (Part 2, Software Configuration Management)," ISO 12220-2

i. ISO 10012-1, "Quality Assurance Requirements for Measuring Equipment: Part 1, Meteorological Confirmation System for Measuring Equipment"

j. "Quality Management: Guidelines on Quality Assurance for Project Management," ISO 10006

k. CJCSI 5716.01 Series, "Remedial Action Project (RAP) Program"

l. Military Standard for Configuration Management, MIL-STD-973

m. "Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS)," DISA Joint Interoperability Engineering Organization (JIEO), DISA

n. DOD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)"

o. CJCSM 6722.01 Series, "Global Command and Control System Configuration Management Plan" **(TO BE WRITTEN)**

GLOSSARY

Part I - Abbreviations and Acronyms

ADP	automated data processing
ADPE	automated data processing equipment
AGSC	Assistant GCCS Site Coordinator
AMHS	Automated Message Handling System
API	application program interface
C2	command and control
C4	command, control, communications, computers
C4I	command, control, communications, computers, and intelligence
C4IFTW	command, control, communications, computers, and intelligence for the warrior
CA	configuration audit
CCB	Configuration Control Board
CI	configuration item
CINC	commander in chief
CJCS	Chairman of the Joint Chiefs of Staff
CJTF	Commander, Joint Task Force
CM	configuration management
CMP	Configuration Management Plan
COE	common operating environment
COTS	commercial-off-the-shelf
C/S/A	CINCs, Services, and Agencies
CSA	configuration status accounting
CSCI	computer software configuration item
CSOD	Command Systems Operations Division
DAA	designated approving authority
DBMS	Data Base Management System
DICO	Data Information Coordination Office
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
ECP	engineering change proposal
FCA	functional configuration audit
GCC	global command and control

GCC	Global Control Center
GCCS	Global Command and Control System
GCCS DIR	GCCS Director
GDBA	GCCS Database Administrator
GMC	Global Command and Control System (GCCS) Management Center
GNA	GCCS Network Administrator
GOTS	government-off-the-shelf
GriD	GCCS Requirements Database
GSA	GCCS System Administrator
GSC	GCCS Site Coordinator
GSO	GCCS Security Officer
HW	hardware
I&RTS	Integration and Runtime Specification
IOC	initial operational capability
IP	internet protocol
IS	information system
ISSO	Information Systems Security Officer
IT	information technology
JCS	Joint Chiefs of Staff
JS(J3)	Joint Staff, Operations Directorate
JS(J6)	Joint Staff, Command, Control, Communications, and Computer Systems Directorate
JS	Joint Staff
JTF	joint task force
JULLS	Joint Uniform Lessons Learned System
LAN	local area network
LCC	local control center
MLS	multi-level security
NCA	National Command Authorities
NMCC	National Military Command Center
OPR	Office of Primary Responsibility
OSD	Office of the Secretary of Defense
OSE	open systems environment
OSF	Operational Support Facility, DISA

PCA	physical configuration audit
POC	point of contact
PR	problem report
PSA	Principle Staff Assistant
RCC	regional control center
RDBMS	Relational Database Management System
SHADE	shared data environment
SIPRNET	Secret Internet Protocol Router Network
SIWG	Systems Integration Working Group
SSA	Software Support Activity
SW	software
TAFIM	Technical Architecture Framework for Information Management
VTC	video teleconference
WAN	wide area network
WIN	Worldwide Military Command and Control System (WWMCCS) Intercomputer Network
WWMCCS	Worldwide Military Command and Control System
WWW	worldwide web

Part II - Definitions

aggregate segment - A collection of segments grouped together, installed, deleted, and managed as a single unit. [DII COE Integration & Runtime Specification (I&RTS, V2.0, OCT 95]

application program interface (API) - (1) The interface, or set of functions, between the application software and the application platform. [APP] (2) The means by which an application designer enters and retrieves information. [DII Master Plan, V5.0, NOV 1996] (3) A programmer's guide that describes the COE software libraries and services, and how to write software modules that interface with and use the COE services. (I&RTS, V2.0, OCT 95]

approved software - Software that has been tested as compatible with the COE. An approved products list might contain Oracle, Sybase, WordPerfect, Kermit, SEWC, NITES, etc. In this context, approved software implies only that the software has been tested and confirmed to work within the environment. It does *not* imply that the software has been approved or authorized by any government agency for any specific system. (I&RTS, V2.0, OCT 95]

automated data processing (ADP) - Recording, filing, computing, and producing of data by means of electronic computers and associated auxiliary equipment. [US Navy ADP Glossary]

Automated Information System (AIS) - Computer hardware, computer software, telecommunications, information technology, personnel, and other resources that collect, record, process, store, communicate, retrieve, and display information. An AIS can include computer software only, computer hardware only, or a combination of the above. [DODD 8000.1]

Automated Message Handling System (AMHS) - The collection of interconnected user agents (UAs), message systems (MSs), and message transfer agents (MTAs) that convey messages from one user to another. The AMHS is designed in accordance with the principles of the reference model of OSI for ITU-T applications (Recommendation x.200) and uses the presentation layer (Layer 6) services offered by other, more general, application service elements. [DISA/D2]

automated tools - Software performing a sequence of operations to assist the user in achieving a goal (e.g., within graphics software, application code, functions that align objects, smooth curves, or draw circles). [HCI Style Guide]

baseline - A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development and that can be changed only through formal change control procedures or a type of procedure such as configuration management. [IEEE STD 610.12]

bootstrap COE - That subset of the COE that is loaded in order to have enough of an operational environment that segments can be loaded. The bootstrap COE is typically loaded along with the operating system though vendor supplied instructions or low level Unix commands such as *tar* and *cpio*. (I&RTS, V2.0, OCT 95]

C4I for the Warrior Vision - The realization of a global command, control, communications, computer, and intelligence system that directly links and supports the warriors -- combat troops of all Services -- who engage in military operations in a rapidly changing world, providing them with accurate and complete pictures of their battlespace, timely and detailed mission objectives, and the clearest view of their targets. [C4IFTW, J6] [DII Master Plan, V5.0, NOV 1996]

change requests - A generic term used to collectively refer to all types of requests that would result in changes in hardware, software/segments, documentation, or functionality. Possible types of change requests are engineering change proposals, new requirements, and proposals for migration systems.

client - A computer program, such as a mission application, that requires a service. Clients are consumers of data while servers are producers of data. (I&RTS, V2.0, OCT 95]

CM Library - The master CM library, maintained by DISA, of all GCCS documents.

commercial-off-the-shelf (COTS) - Refers to an item of hardware or software that has been produced by a contractor and is available for general purchase. Such items are at the unit level or higher. Such items

must have been sold and delivered to government or commercial customers, must have passed customer's acceptance testing, and must be operating under the customer's control and within the user environment. Further, such items must have meaningful reliability, maintainability, and logistics historical data. [TAFIM 2.0, vol 1]

common operating environment (COE) - The DII COE establishes an integrated software infrastructure which facilitates the migration and implementation of functional mission applications and integrated databases across information systems in the Defense Information Infrastructure. The DII COE provides architecture principles, guidelines, and methodologies that assist in the development of mission application software by capitalizing on a thorough, cohesive set of infrastructure support services. The DII COE specification is derived from the complete TAFIM. [DII Master Plan, V5.0, NOV 1996]

compliance - A numeric value, called the compliance level, which measures the degree to which a segment conforms to the principles and requirements defined by COE standards and the degree to which the segment makes use of COE services. Compliance is measured in four areas, called compliance categories. The four categories are Runtime Environment, Architectural Compatibility, Style Guide, and Software Quality. (I&RTS, V2.0, OCT 95]

configuration - Functional and physical characteristics of a product as defined in technical documents and achieved in the product. [ISO STD 10007:1995]

configuration audit - Examination to determine whether a configuration item conforms to its configuration documents. [ISO STD 10007:1995]

configuration baseline - Configuration of a product, formally established at a specific point in time, which serves as a reference for further activities. [ISO STD 10007:1995]

configuration control - Activities comprising the control of changes to a configuration item after formal establishment of the configuration documents. [ISO STD 10007:1995]

Configuration Control Board (CCB) - Group of technical and administrative experts with the assigned authority and responsibility to make decisions on the configuration and its management. [ISO STD 10007:1995]

configuration documents - Documents that define the requirements, design, build/production, and verification for a configuration item. [ISO STD 10007:1995]

configuration identification - Activities comprising determination of the product structure, selection of the configuration items, documenting the configuration item's physical and functional characteristics including interfaces and subsequent changes, and allocating identification characters or numbers to the configuration items and their documents. [ISO STD 10007:1995]

configuration item (CI) - Aggregation of hardware, software, processed materials, services or any of its discrete portions that is designated for configuration management and treated as a single entity in the configuration management process. [ISO STD 10007:1995]

configuration management (CM) - [1] Technical and organizational activities comprising: configuration identification; configuration control; configuration status accounting; and configuration auditing. [ISO 10007:1995]. [2] A discipline applying technical and administrative direction and surveillance to: (a) identify and document the functional and physical characteristics of a configuration item, (b) control changes to those characteristics, and [c] record and report changes to processing and implementation status. [MIL-STD 973]

Configuration Management Plan (CMP) - Document setting out the organization and procedures for the configuration management of a specific product or project. [ISO STD 10007:1995]

configuration status accounting (CSA) - (1) Formalized recording and reporting of the established configuration documents, the status of proposed changes and the status of the implementation of approved changes. [ISO STD 10007:1995]

conformance - Meeting standards. By running standard test scripts, conformance testing ensures that a product meets standards. [TAFIM 2.0, vol 4]

data - Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned.

database - Structured or organized collection of information which may be accessed by the computer. [HCI Style Guide]

Database Management System - Computer application program that accesses or manipulates the database. [HCI Style Guide]

defense information infrastructure (DII) - A seamless web of communications networks, computers, software, databases, applications, and other capabilities that meets the information processing and transport needs of DOD users in peace and in all crises, conflict, humanitarian support, and wartime roles. [DII Master Plan, V5.0, NOV 1996]

Defense Information System Network (DISN) - A subelement of the DII, the DISN is the DOD's consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner. [DII Master Plan, V5.0, NOV 1996]

Data Information Coordination Office (DICO) - The Director for Operations (J-3), Joint Staff, will designate a Data Information Coordination Office (DICO) to provide operational direction and guidance for the GCCS.

distributed database - (1) A database that is not stored in a central location but is dispersed over a network of interconnected computers. (2) A database under the overall control of a central database management system but whose storage devices are not all attached to the same processor. (3) A database that is physically located in two or more distinct locations. [FIPS PUB 11-3]

distributed system - A system consisting of a group of connected, cooperating computers. [TAFIM 2.0, vol 4]

embedded user functionality - Embedded user functionality are those DII COE (non-COTS) applications/segments that provide mission functions required for users to do their jobs. These applications involve user issues, not just technical issues, that can significantly impact the way users do their jobs. Embedded user functionality is subject to more

stringent oversight and controls by the GCCS CCB than are the COTS portions of the DII COE.

Engineering Change Proposal (ECP) - A proposed change to current approved GCCS joint mission area application configuration item(s) (CIs), and the documentation by which the change is described, justified, and submitted to the GCCS CCB and GCC Management Structure for approval or disapproval. An ECP is a request to change a CI specification or functional requirement, usually to enhance or supplement the functionality of the CI or system.

environment - In the context of the COE, all software that is running from the time the computer is rebooted to the time the system is ready to respond to operator queries after operator login. This software includes the operating system, security software, installation software, windowing environment, COE services, etc. The environment is subdivided into a runtime environment and a software development environment. (I&RTS), V2.0, OCT 95]

evolutionary build - The practice of placing agreed-upon functional or technical requirements into a build package that will become a version baseline for a system.

end user - Person who ultimately uses the computer application or output. [HCI Style Guide]

function - Appropriate or assigned duties, responsibilities, missions, tasks, powers, or duties of an individual, office, or organization. A functional area is generally the responsibility of a PSA (e.g., personnel) and can be composed of one or more functional activities (e.g., recruiting), each consisting of one or more functional processes (e.g., interviews). [Joint Pub 1-02, DoDD 8000.1, and DoD 8020.1-M]

functional configuration audit (FCA) - A formal examination to verify that a configuration item has achieved the performance and functional characteristics specified in its configuration documents. [ISO STD 10007:1995]

Global Command and Control System (GCCS) - A highly mobile, deployable command, control, communications, computers, and intelligence (C4I) system that supports forces for joint and combined operations throughout the spectrum of conflict anytime and anywhere in

the world with compatible, interoperable, and integrated C4I systems. [DII Master Plan, V5.0, NOV 1996]

GCCS Database Administrator (GDBA) - The GDBA is responsible for the day-to-day operations of the databases located at the GCCS site. This may include the primary database server (Sun Sparc 1000 or Sparc 2000) running the Oracle RDBMS, or the Executive Manager application using the Sybase RDBMS, or the AMHS server application using the Verity Topic RDBMS.

GCCS Designated Approving Authority (DAA) - The Director for Command, Control, Communications, and Computer Systems, (J-6), Joint Staff, is the designated approving authority (DAA) for all GCCS security matters. The GCCS DAA is responsible for approving security policies, providing security guidance, and taking whatever actions are necessary to ensure the integrity and security of the GCCS operations.

GCCS Director (GCCS DIR) - The Director for Command, Control, Communications, and Computers (J-6), Joint Staff, will designate a GCCS Director (GCCS DIR). The GCCS DIR will be the focal point for all aspects of GCCS operations related to system and network configuration, fault, performance, and security management. This responsibility includes testing, evaluation, and implementation of the GCCS. The GCCS DIR will provide technical solutions to the DICO for an operational decision on global GCCS problems or recommended changes.

Global Command and Control System (GCCS) Management Center (GMC) - The GMC will be a collection of offices functioning under a single management umbrella. This collection of offices will use a combination of COTS and GOTS system and network management applications to continually monitor the health of the GCCS. The GMC Pentagon will support the activities of all the GCCS sites, the National Military Command Center (NMCC), and the functions of the JS/J6 GCCS DIR.

GCCS Network Administrator (GNA) - The GNA is responsible for the day-to-day operation of the GCCS LAN, the data and applications servers, the communications devices (premise router, communications server, and intelligent hubs) and related GCCS equipment.

GCCS Security Officer (GSO) - The Director for Command, Control, Communications, and Computers (J-6), Joint Staff, will designate a GCCS Security Officer (GSO). The GSO is responsible for the day-to-day security operations of the GCCS. As such, all site GCCS Information

System Security Officers (Site GCCS ISSOs) will be responsible to the GSO. The GSO is responsible for providing security information and recommendations to the Joint Staff DAA for matters involving the GCCS.

GCCS Site(s) Coordinator (GSC) - The GSC is responsible for coordinating all system and network support activities within the GCCS site. The individual filling this role will be the primary focal point for coordinating with the GMC and other GCCS organizations. One of the major duties of this position will be to direct activities during and following an emergency condition to minimize the loss of GCCS mission capabilities at the site.

GCCS System Administrator (GSA) - The GSA is responsible for a variety of duties with the major focus being on maintaining the GCCS applications, providing local user support, and troubleshooting site problems associated with the GCCS applications. This includes the responsibility for determining if the GCCS applications are properly storing correctly formatted data to the GCCS database servers.

GMC Help Desk - The GMC-Help Desk is the GCCS user's primary point of contact for all problems associated with the joint mission pertaining to hardware, software, network, or communications. The GMC-Help Desk will not be responsible for supporting C/S/A unique applications. Users should coordinate with their GCCS Site Coordinator/Service Help Desk to verify a problem really exists prior to contacting the GMC-Help Desk.

government-off-the-shelf (GOTS) - Software products that have been developed by the government and distributed throughout the government for use. [DII Master Plan, V5.0, NOV 1996]

hardware - (1) Physical equipment, as opposed to programs, procedures, rules, and associated documentation. (2) Contrast with software. [FIPS PUB 11-3]

information - Any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. [OMB Circular A-130]

Information System (IS) - A system consisting of mission specific or functional applications, data, and technical architecture consisting of support applications, application platforms, and the external environment including devices such as terminals, printers, and communications networks. [TAFIM 2.0, vol 1]

information technology (IT) - The technology included in hardware and software used for Government information, regardless of the technology involved, whether computers, communications, micro-graphics, or others. [OMB Circular A-130 and DoDD 8000.1.]

infrastructure - Infrastructure is used with different contextual meanings. Infrastructure most generally relates to and has a hardware orientation but note that it is frequently more comprehensive and includes software and communications. Collectively, the structure must meet the performance requirements of and capacity for data and application requirements. Again note that just citing standards for designing an architecture or infrastructure does not include functional and mission area requirements for performance. Performance requirement metrics must be an inherent part of an overall infrastructure to provide performance interoperability and compatibility. It identifies the top-level design of communications, processing, and operating system software. It describes the performance characteristics needed to meet database and application requirements. It provides a geographic distribution of components to locations. The infrastructure architecture is defined by the service provider for these capabilities. It includes processors, operating systems, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs. [DoD 8020.1-M]

initial operational capability (IOC) - (1) At the system level, IOC is the point at which some portion of the technical and operational specifications defined by the requirements documents have been achieved. The specific definition of IOC will vary for each system and would be negotiated between the PM, the user, and the O&M activity. (2) At the site level, IOC is the point at which the technical specifications of that portion of the system installed at a specific site meet the documented requirements, but some portion of testing and/or operational specifications remains to be accomplished. The specific definition of IOC is site specific and would be negotiated between the PM, the site manager, and the O&M activity. [DISA/D4]

interface - A connecting link or interrelationship between two systems, two devices, two applications, or the user and an application, device, or system. In the OSI Reference Model, it is the boundary between adjacent layers. [TAFIM 2.0, vol 4]

Joint Universal Lessons Learned System (JULLS) - A formatted data base program which allow users to input, access and manipulate automated lessons learned. There are three types of JULLS records in the database: 1) Lessons Learned JULL - deals with a specific item noted during an exercise or operation; 2) Summary JULL - provides an overall picture of the objectives and results of an exercise or operation; 3) Assessment JULL - reports on the degree of success obtained from the testing of specific exercise objectives.

kernel COE - That subset of the COE component segments which is required on all workstations. As a minimum, this consists of the operating system, windowing software, security, segment installation software, and an Executive Manager. (I&RTS, V2.0, OCT 95]

Local Area Network (LAN) - A data network, located on a user's premises, within a limited geographic region. Communication within a local area network is not subject to external regulation; however, communication across the network boundary may be subject to some form of regulation. [FIPS PUB 11-3]

mission area variant - A collection of segments which are relevant to a particular mission area (e.g., analysis, planning). A mission area variant is typically a list of workstation variants. (I&RTS, V2.0, OCT 95]

National Command Authorities (NCA) - The President and the Secretary of Defense or their duly deputized alternates or successors.

open architecture - A term used to describe any computer or peripheral design that has published specifications. A published specification lets third parties develop add-on hardware for an open-architecture computer or device. The term can also refer to a design that provides for expansion slots on the motherboard, allowing the addition of boards to enhance or customize a system.

open system - A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software: (1) to be ported with minimal changes across a wide range of systems, (2) to interoperate with other applications on local and remote systems, and (3) to interact with users in a style that facilitates user portability. [P1003.0/D15]

open systems environment (OSE) - The comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles. [P1003.0/D15]

platform - The entity of the Technical Reference Model that provides common processing and communication services that are provided by a combination of hardware and software and are required by users, mission area applications, and support applications. [TA]

physical configuration audit (PCA) - A formal examination of the "as-built/produced" configuration of a configuration item to verify that it conforms to its product configuration documents. [ISO STD 10007:1995]

portability - (1) The ease with which a system or component can be transferred from one hardware or software environment to another. [IEEE STD 610.12] (2) A quality metric that can be used to measure the relative effort to transport the software for use in another environment or to convert software for use in another operating environment, hardware configuration, or software system environment. [IEEE TUTOR] (3) The ease with which a system, component, data, or user can be transferred from one hardware or software environment to another. [TA]

Problem Report - A PR is a notification that a CI is not performing to its functional specification(s). A CI may be a segment, application, application module, interface, documentation, etc. PRs are also known as Global Command and Control System PRs or GSPRs.

Relational Database Management System (RDBMS) - An automated system for managing databases whose structure tables have the following properties: (1) each row in the table is distinct from every other row; (2) each row contains only atomic data, that is, there is no repeating data or such structures as arrays; (3) each column in the relational table defines named data fields or attributes.

remote install - The ability to electronically install segments from a local site (such as the DISA Operational Support Facility) to a remote site (such as USACOM). In a "push" mode, the local site initiates and controls the segment installation. In a "pull" mode, the remote site initiates and controls the segment installation. (I&RTS, V2.0, OCT 95]

router - Generically, any machine responsible for making decisions on which path, out of several different paths, network traffic will follow. [Comer] [DISA/DO3 (CIO)]

runtime environment -The runtime context determined by the applicable account group, the COE, and the executing segments. (I&RTS, V2.0, OCT 95]

scalability - The ability to use the same application software on many different classes of hardware/software platforms from personal computers to super computers (extends the portability concept). [USAICII] The capability to grow to accommodate increased work loads.

seamless interface - Ability of facilities to call one another or exchange data with one another in a direct manner. Integration of the user interface that allows a user to access one facility through another without any noticeable change in user interface conventions. [DSAC SYS IM]

segment - (1) A segment is a module of related software that performs a function or set of functions. (2) A collection of one or more CSCIs (Computer Software Configuration Items) most conveniently managed as a unit. Segments are generally defined to keep related CSCIs together so that functionality may be easily included or excluded in a variant. (I&RTS, V2.0, OCT 95]

server type -A class of servers in a client/server architecture. Among the different types of servers are the following: Name, Directory, Authentication, Access Control, Cryptographic, Communications, Time, File, Data, Print, Mail, Electronic Data Interchange (EDI), Applications, Presentation, and Sensor Monitor/Actuator. [TAFIM 2.0, vol 4]

shared data environment (SHADE) - The SHADE is the standards-based architecture that supports one-time data entry through reusable Information Technology/data assets and standard data elements. SHADE consists of two components: (1) shared distributed databases of standard data structures and standard data. (2) infrastructure components which include shared data dictionary services, transformation software, interfaces, and data warehouses. [DII Master Plan, V5.0, NOV 1996]

SIPRNET - The data communications component of the DISN used for SECRET data. SIPRNET uses the same Internet Protocol routing

technology as in NIPRNET with additional security measures needed to protect classified data transmissions.

Site GCCS designated approving authority (Site GCCS DAA) - The Site GCCS DAA is responsible for local security policies and guidance to ensure the integrity and security of the GCCS operations are maintained. The Site GCCS DAA is responsible for accrediting GCCS at the site.

Site GCCS Information System Security Officer (Site GCCS ISSO) - The Site GCCS ISSO is responsible for ensuring the integrity and security of the local GCCS system and network. The Site GCCS ISSO is responsible for providing security information to the Site GCCS DAAs. The GMC will be supported by the Site GCCS ISSO appointed at these locations.

site variant - A collection of segments that are relevant to the mission needs of a specific site (e.g., CVN, TRANSCOM, CJTF). A site variant is typically a list of mission area variants. (I&RTS, V2.0, OCT 95]

Software Support Activity (SSA) - A DISA DII COE support organization which enters software segments into an online library for configuration management and confirms DII compliance. The SSA then tests interaction between segments and the impact on performance, memory utilization, etc. (I&RTS, V3.0, JAN 97]

system software - Computer programs that control, monitor, or facilitate the use of an Automated Information System; for example, operating systems, programming languages, communications, input-output control, sorts, security packages, and other utility programs. Includes off-the-shelf application packages obtained from manufacturers and commercial vendors such as for word processing, spreadsheets, database management, graphics, and computer-aided design. [Joint Pub 6-02.1]

system variant - A collection of segments that are relevant to a specific defined mission area (e.g., C4I, logistics, finance). GCCS and GCSS are two examples of a system variant. A system variant is typically a list of site variants. (I&RTS, V2.0, OCT 95]

Technical Architecture Framework for Information Management (TAFIM) - The TAFIM is a set of documents produced by DISA for the OSD to guide DOD information systems toward an open systems architecture. It provides the services, standards, design concepts, components, and configurations that can be used to guide the

development of technical architectures that meet specific mission requirements. [TAFIM 2.0, vol 1]

user - (1) Any person, organization, or functional unit that uses the services of an information processing system. (2) In a conceptual schema language, any person or any thing that may issue or receive commands and messages to or from the information system. [FIPS PUB 11-3]

variant - A subset of the superset of all software. This subset includes the COE and is fielded to service an operational mission area. A variant represents that collection of segments, including COE component segments, that are suitable for a particular site, mission area, or workstation. (I&RTS, V2.0, OCT 95]

video teleconferencing (VTC) - A means of televising and transmitting a meeting between two or more organizations. [JITC Dictionary]

Worldwide Military Command and Control System (WWMCCS) - Provides the NCA, CJCS, and the commanders of the unified commands with the means for planning, directing, and controlling US military forces worldwide. WWMCCS ADP, a subset of WWMCCS, was the first comprehensive automated operational planning and execution support for joint C2 support. WWMCCS ADP was built upon proprietary Honeywell mainframe/minicomputer hardware and software, with accompanying Top-Secret level secure RF and landline interconnectivity. WWMCCS ADP is in the process of being replaced by a modern client-server automated system, GCCS and GCCS-T.